BIG DATA AND ARTIFICIAL INTELLIGENCE – EVOLVING MARKET MISCONDUCT RISKS

Commentary on big data and artificial intelligence risk has tended to focus on the risks associated with treating data subjects and customers unfairly or unlawfully, principally under GDPR. There has been less focus on new wholesale market misconduct risks. That is surprising given the exponential growth in the use of alternative data and AI in the financial markets and given the regulatory focus on market misconduct since the financial crisis.

On 13 February 2019 Julia Hoggett, Director of Market Oversight at the FCA, gave a speech to AFME in which she remarked on the evolving market misconduct risks associated with big data and AI. Firms and senior managers need to understand these new risks which can give rise to serious criminal and civil liability.

In this briefing we consider two specific risks: insider dealing risk associated with big data and the manipulation risks associated with AI.

We focus on the risks under the EU Market Abuse Regulation ("MAR") but given the potential territorial reach of MAR the risks are likely to be relevant to firms outside the EU, and the underlying issues are likely to be of relevance in other market misconduct regimes too.

ALTERNATIVE DATA INSIDER DEALING RISK

Buy-side firms have been using data analytics to inform trading decisions for many years. But data science, big data and machine learning are now becoming essential to compete. Both buy-side and sell-side firms have been investing heavily in identifying new datasets and new technology for data analysis.

Alternativedata.org, a website run by a group of former buy-side and sell-side analysts containing information relating to the alternative data market, records that the total buy-side spend on alternative data in 2017 was $400m, with this expected to rise to $1.7billion by 2020. The total number of buy-side employees has grown 450% in the last five years. The highest grossing data source is credit / debit card data with the most commonly-used data types shown as follows:

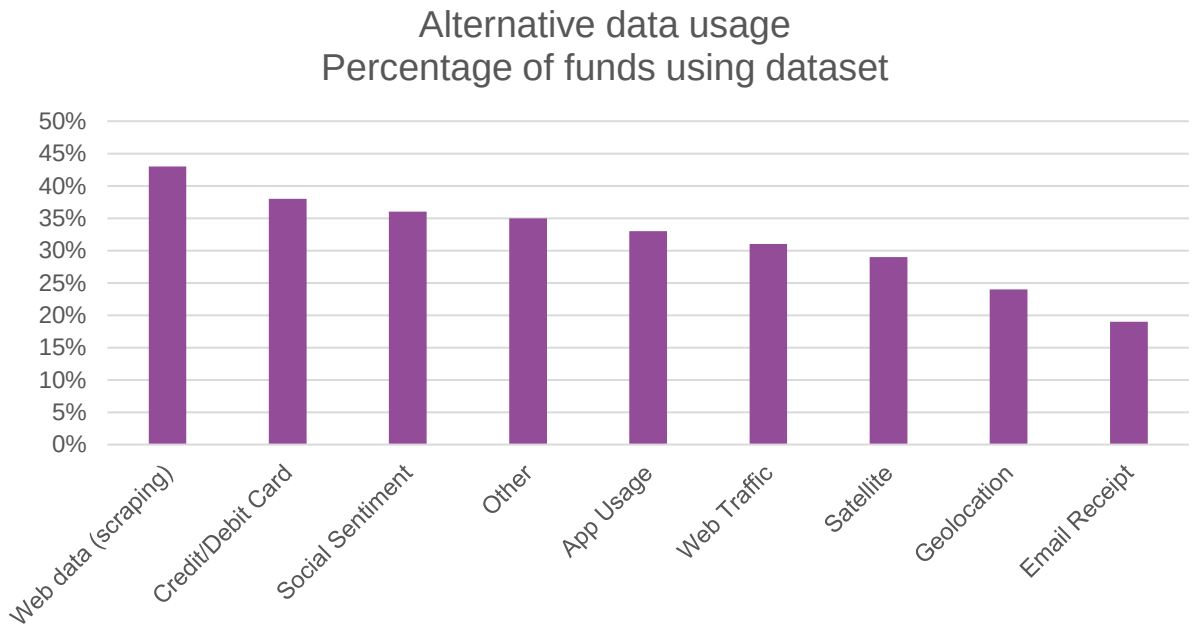
Key points

Big data and insider dealing

- Use of big data or alternative data analysis in wholesale markets has created new forms of insider dealing risk.
- With such intense public focus on the misuse of data, we expect to see increased pressure on regulators to act against firms who are perceived to obtain unfair advantage in the financial markets through use of big data.
- Firms using datasets, or providing them to others, need to have systems in place to ensure that they do not contain, and are not derived from, inside information, which may involve assessing whether data has been obtained or processed in breach of privacy obligations, including under GDPR.

AI and manipulation

- Use of AI in trading gives rise to the risk of market manipulation. There has already been enforcement action in relation to use of algorithms designed to manipulate the market.
- With the growth of machine learning firms need also be aware of the risk that algorithms may unintentionally "learn" manipulative behaviour. The EU market abuse regime does require market manipulation to be intentional.
- Firms also need to look beyond algorithmic trading. Manipulation can occur through dissemination of false or misleading information. Use of AI in to generate published material, for example in generating research or target prices, gives rise to a high manipulation risk. Where such material is misleading, even if unintentionally, the firm may commit market manipulation. Firms need to have systems in place to ensure that the information published is accurate and not misleading.



Source: Alternativedata.org

In her speech to AFME, Julia Hoggett drew attention to evolving market misconduct risks associated with use of such alternative data:

We have traditionally focused on company results and announcements, news flows and analysts reports to determine how one might think about inside information and publicly available information. However, a world where we create data at an ever-increasing pace, must lead us to consider how we view these new data sources, especially when they have the potential to be market moving.

Using such data to provide new insights into the performance of companies and markets is a valuable addition to the price formation process. However, as a result, there will no doubt be interesting regulatory questions we will have to ask ourselves in the future. We will be exploring how data is used in wholesale markets as we explore that question.

In other words, as we create more electronic data, it is becoming increasingly difficult to distinguish between data which is publicly available and data which is non-public and therefore potentially inside information.

"As we create more electronic data, it is becoming increasingly difficult to distinguish between data which is publicly available and data which is non-public and therefore potentially inside information."

Knowing when data is publicly available

In the EU under the Market Abuse Regulation, information may be deemed "publicly available" if it is capable of being accessed legitimately, even if that information is not readily accessible by everyone. It is not relevant that the information is only available through observation or analysis by a person with above average financial resources, expertise or competence. Thus, for example, it can be permissible to trade on analysis of privately-obtained satellite imagery because the images are observable from a public place, even if only by those with significant financial resources.

FCA guidance provides that in assessing whether information is publicly available the FCA will also consider whether the information can be obtained without infringing rights or obligations of privacy, property or confidentiality.

In the context of alternative electronic data, assessing whether information has been or can be obtained in breach of confidentiality or privacy is becoming increasingly difficult.

For example, where an app collects data relating to user spending patterns at a listed online retailer and that data is then anonymised, aggregated and sold for use in trading decisions relating to the retailer's shares, is that information publicly available as effectively equivalent to traditional footfall analysis? Or is it non-public and therefore potentially inside information?

The data privacy rights of the app user may have been infringed if the data has been processed unlawfully. Processing in this context has a broad meaning, encompassing almost all forms of use. Lawful processing generally requires specific and informed consent. If the app user has not given consent for spending data to be processed for these specific purposes, the data may have been processed in breach of rights of privacy which could be relevant to the question of whether the ultimate dataset constitutes inside information.

It follows that it may not be sufficient for firms simply to assess whether data itself is "scrubbed" of private or confidential data. Depending on the nature of the data it may also be necessary to consider whether privacy or confidentiality rights were breached at any earlier stage in the creation of the dataset.

With such intense public focus on the loss and misuse of data more broadly, we expect to see increased pressure on regulators to act against firms who are perceived to give or obtain unfair advantage in the financial markets through privileged access to big data gathered from consumers.

Such cases could involve parallel investigations by data protection authorities in relation to underlying breaches of data protection principles. It is noteworthy that the amended Memorandum of Understanding between the FCA and the Information Commissioner's Office (ICO) published on 19 February 2019 contains new paragraphs specifically contemplating parallel investigations and addressing information sharing in that context.

"With such intense public focus on the loss and misuse of data we expect to see increased pressure on regulators to act against firms who are perceived to obtain unfair advantage in the financial markets through privileged access to big data."

Private polling

We have already seen growing pressure in this area in relation to the use of private polls by hedge funds. The UK Treasury Select Committee has written to the FCA asking how such private polls are lawful. A central issue there is whether such polling data should be considered "publicly available" when, in practice, only a few have privileged access to it. The conventional view is that such polls are deemed to be publicly available because the poll has been conducted in public without infringing rights of privacy or confidentiality. But can that be true if the persons polled have not specifically consented to the purposes for the poll data would be processed? The answer is unclear.

At a Treasury Select Committee hearing on 15 January 2019 Andrew Bailey was asked what action the FCA is taking on private polls. He explained that the FCA is giving thought to whether it can usefully address the issue by publishing guidance. Such guidance would likely come in the form of an amendment to the FCA's Code of Market Conduct and could extend to the use of alternative data generally and the circumstances in which such data should be deemed publicly available.

"We have already seen growing pressure in relation to the use of private polls. A central issue there is whether such polls should be considered "publicly available" when, in practice, only a few have privileged access."

Systems and controls

Firms are required to have systems and controls in place to prevent and detect market misconduct by themselves and clients. Senior managers are required to take responsibility for these systems and controls and (as recent changes to the Financial Crime Guide make clear) are expected to understand the legal definitions of insider dealing and market manipulation and the ways in which the firm may be exposed to the risks. Systems and controls must be adequate to address differences between jurisdictions: generic global systems are unlikely to be adequate.

Those selling or using alternative data will be expected to have processes in place to understand the content and provenance of datasets and to take reasonable steps to ensure that the data has been obtained and processed lawfully. Firms whose clients use alternative data may be expected to conduct due diligence to satisfy themselves that the dataset contains or is based on publicly available information. Firms will need to adjust their systems to take account of any amended guidance from the FCA as to when data should be considered publicly available.

AI AND MANIPULATION RISK

There are separate but no less serious manipulation risks associated with growing use of AI.

In the same speech to AFME on 13 February 2019, Julia Hoggett also said:

I can see a world where seemingly 'rational' AI, unconstrained and exposed to certain markets and data, would deem it entirely rational to commit market manipulation. Now, the FCA cannot prosecute a computer, but we can seek to prosecute the people who provided the governance over that computer.

Algorithmic trading is a thoroughly embedded part of how markets function now and is it continuing to evolve. How machine learning and AI are applied to trading activity is something that we must closely follow, not just to understand

how markets function and ensure that they function well, but also to scan for potentially unintended consequences.

Manipulative algorithmic trading has received significant attention for several years. The three most recent cases in the UK have been:

- The August 2015 High Court decision in FCA v Da Vinci Invest and Others [2015] EWHC 2401 (Ch) in which the FCA successfully obtained penalties in the High Court against the defendants for spoofing using an algorithm.
- The 2016 High Court decision in extradition proceedings against Navinder Sarao (the Hound of Hounslow) who subsequently pleaded guilty to spoofing of the market for "E-minis" – a stock market index futures contract based on the Standard & Poors 500 Index - on the CME, operating from his residence in the UK, using an algorithm.
- The November 2017 FCA Final Notice against Paul Axel Walter who was fined £60,090 for committing market abuse by placing orders which would advance the best bid or best offer, attracting algorithms to follow, before cancelling his own orders.

"Manipulation by AI need not be confined to order behaviour such as spoofing, nor would it need to be to "deliberate" to constitute market manipulation"

The risk for the future, to which Julia Hoggett referred in her speech, is that algorithms designed to behave in a legitimate way over time through AI and machine learning come to manipulate as an alternative means of "successfully" achieving the objectives set to them.

Such manipulation by AI need not be confined to order behaviour such as spoofing as in the three cases highlighted above, nor would it need to be confined to "deliberate" conduct by the AI in question to constitute market manipulation.

Where trading decisions are taken by or driven by AI, firms need to understand the strategies the AI is intended to effect and to have processes in place to monitor trading activity to ensure that it is consistent with those strategies. Is the strategy constant or can it evolve? If so what is the risk of behaviour becoming manipulative.

Beyond algorithmic trading

Firms also need to look beyond algorithmic trading. Manipulation can occur through dissemination of false or misleading information. Use of AI to generate published material, for example in generating research (e.g. to meet the cost pressures associated with MIFID II) or target prices, gives rise to a high manipulation risk.

"Use of AI to generate published material, for example in generating research (e.g. to meet the cost pressures associated with MIFID II) or target prices, gives rise to a high manipulation risk."

Where such material is misleading, even if unintentionally, the firm may commit market manipulation.

The FCA has commented recently on the risks associated with automated research and robo advice, while also acknowledging its potential to boost competition in the UK financial advice market. The FCA stated that it is monitoring developments in this area and reiterated that a firm's responsibility for a model will not be reduced where the firm uses third party suppliers to help with the technology side.

CONTACTS

Oliver Pegden
Senior Associate

T +44 (0) 20 7006 8160
E oliver.pegden
@cliffordchance.com

Caroline Dawson
Senior Associate

T +44 207006 4355
E caroline.dawson
@cliffordchance.com

Oliver Pegden is a senior associate in our regulatory Enforcement team specialising in market misconduct cases. He was seconded to the FCA during 2014 and 2015 where he was a lawyer in the team responsible for FCA v Da Vinci Invest and Others [2015] EWHC 2401 (Ch) in which the FCA successfully obtained penalties in the High Court against the defendants for market abuse using "spoofing" or "layering" using an algorithm.

Caroline Dawson is a senior associate in our Financial Regulation team with a focus on market misconduct and regulation of trading and investment research. She was seconded to the equities legal team of a global investment bank in 2009 and to the Bank of England in 2014 and has advised a wide range of market participants on implementation of MiFID2 and the EU Market Abuse Regulation.